

JUN. 12. 2006 12:27PM

16509618301

RECEIVED
CENTRAL FAX CENTER

NO. 633 P. 4

JUN 12 2006

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Kobayashi, Osamu

Attorney Docket No.: GENSP151C1

Application No.: 10/813,346

Examiner: Sherkat, Arezoo

Filed: March 29, 2004

Group: 2131

Title: DISPLAY UNIT STORING AND USING A
CRYPTOGRAPHY KEY

Confirmation No.: 5003

CERTIFICATE OF FACSIMILE TRANSMISSION

I hereby certify that this correspondence is being transmitted by facsimile to fax number 571-273-8300 to the U.S. Patent and Trademark Office on June 12, 2006.

Signed: _____

Linda L. Quintana

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicant hereby requests review of the rejections in the above-identified application. This request is being filed with a Notice of Appeal. Review is requested for the reasons stated in the accompanying remarks.

BEST AVAILABLE COPY

REMARKS

For the purpose of this PRE-APPEAL BRIEF REQUEST FOR REVIEW only, the Applicant sets forth claim 1 immediately below as a representative claim. In specific instances below, the Applicant also addresses features recited in other claims, including claims dependent on claim 1. The Applicant reserves the right to argue each claim separately when and if an Appeal Brief is eventually filed.

1. A method of using a number of a plurality of cryptographic keys in a display device having a printed circuit board (PCB) and a master block, comprising:
 - providing the number of the plurality of keys to the PCB by the master block;
 - selecting one of a number of available encryption protocols for each of the provided keys;
 - encrypting each of the provided keys based upon a particular one of the selected encryption protocols;
 - storing the encrypted keys in a non-volatile memory by the PCB;
 - decrypting the stored encrypted key, as needed, by the PCB based upon the selected encryption protocol.

Summary of Subject Matter of Claim 1 and Summary of Allegation of "Clear Error"

According to the subject matter of claim 1, a method is provided of using a plurality of cryptographic keys in a display device having a printed circuit board (PCB) and a master block. A number of a plurality of keys are first provided to the PCB by the master block. One of a number of available encryption protocols is then selected for each of the provided keys. It is important to note that the encryption protocol is selected on a per-key basis, thus potentially allowing a different encryption protocol to be used for each key to be encrypted. Each of the keys is then encrypted according to a particular selected encryption protocol. The encrypted keys are then stored in a non-volatile memory. When needed, a stored encrypted key can be decrypted according to a decryption protocol corresponding to the selected encryption protocol used to encrypt that key.

While not the only distinction, the underlined portions in the previous paragraph represent a distinction over the cited references that the Applicant has repeatedly argued is not taught, or suggested by, the cited references. Not only has the Examiner not addressed this

distinction, but also the Applicant has provided clear arguments as to why this distinction is an actual one that makes the subject matter of claim 1 patentable over the cited reference.

The clear error in the Examiner's rejection is discussed in greater detail in the next section.

Detailed Discussion of Clear Error in the Examiner's Rejection of Claim 1

Claim 1 (as well as all other claims) remains rejected as being obvious over High-bandwidth Digital Content Protection System, Revision 1.0 by Intel Corporation (HDCP Revision 1.0 hereinafter) in view of U.S. Patent 5,142,578 issued to Matyas et al. The reviewers are respectfully referred to the Applicant's complete Remarks on pages 6- 8 of Amendment B After Final, filed March 9, 2006. A recap is provided here.

While not the only distinction, the underlined portion set forth above, and repeated here, validates ... that the encryption protocol is selected on a per-key basis, thus potentially allowing a different encryption protocol to be used for each key to be encrypted. This is a distinction that the Applicant has repeatedly argued but that the Examiner has not addressed. While the clear error in the Examiner's rejection is discussed in detail in the next section, the Applicant provides herewith a fragment of the communication to give the reviewers the essence of the clear error; though the reviewers are, again, referred to the Applicant's complete Remarks on pages 6- 8 of Amendment B After Final.

In Amendment B After Final, Applicant states (on page 7) that claim 1 clearly teaches a method that provides "for a selection of one of a number of available encryption/decryption protocols to encrypt the keys, the selection of which is unknown to any outside agent." In stark contrast, in both of the cited references, there is but a single encryption protocol used to encrypt the cryptographic keys at a given cryptographic facility. This is evident in the HDCP reference starting on page 6, first paragraph, describing the authentication protocol, and more particularly, in section 2.2 describing an authentication protocol relying upon a single encryption/decryption protocol that uses the single 40 bit binary KSV that is assigned to the device.

In the Final Office Action (at page 2 lines 10- 11 of the Office Action mailed February 15, 2006), referring to the Matyas reference, the Examiner clearly states "decrypting the stored encrypted key, as needed, by the PCB based upon the selected encryption protocol (i.e., KMb.C6 is formed as the exclusive OR product of the master key, KMb, stored in CF 30' and control vector C6)." Therefore, the Examiner has clearly affirmed that the received key is encrypted with the key KMb.C6. The Applicants are in agreement that Matyas teaches that the key, K, produced by the GKSP (see column 10 lines 8- 9) and transmitted to the receiving cryptographic system, is extracted from keyblk and encrypted with KMb.C6. However, nowhere does Matyas

disclose nor even remotely suggest that there are other encryption protocols besides KMB.C6 that can be used to encrypt the received keys. This is in stark contrast to the invention as recited in claim 1 requiring that one of a number of encryption protocols be selected for each of a number of keys.

Moreover, also in the Final Office Action, the Examiner states:

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of HDCP Revision 1.0 with teachings of Matyas because it would allow to include securely recovering the distributed key-encrypting key by the recipient by decrypting the received key record using the same public key algorithm and private key associated with the public key and re-encrypting the key-encrypting key under a key formed by arithmetically combining the recipient's master key with a control vector contained in the control information of the received key record as disclosed by Matyas.

Furthermore, in the Advisory Action mailed March 29, 2006, the Examiner states, in part:

The type and usage attributes assigned by the originator of the key-encrypting key in the form of a control vector are cryptographically coupled to the key-encrypting key such that the recipient may only use the received key-encrypting key in a manner defined by key generator.

In both of these statements, the Examiner has not properly responded to or otherwise addressed the Applicant's stated contention that claim 1 discloses selecting one of a number of encryption protocols for each of the keys to be encrypted. The Examiner's statement echoes the Applicant's assertion (page 6 of Amendment B After Final) that Matyas merely "assures that the proper recipient has received the appropriate key and does not teach nor remotely suggest that the keys themselves are encrypted/decrypted based upon a selected one of a plurality of available encryption/decryption protocols."

Clear Error in the Examiner's Rejection of the Other Independent Claims

With regard to independent claim 12, for the purpose of this PRE-APPEAL BRIEF REQUEST FOR REVIEW only, the Applicant respectfully submits that the Examiner is in clear error with respect to the rejection of the remaining independent claim 12 for similar reasons discussed above for independent claim 1.

In particular, claim 12 specifically requires:

computer code for selecting one of a number of encryption protocols available to the PCB;

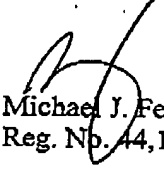
computer code for encrypting the key based upon the selected encryption protocols.

In addition, for the purpose of this PRE-APPEAL BRIEF REQUEST FOR REVIEW only, Applicant respectfully submits that the Examiner is in clear error with respect to the rejection of the dependent claims for reasons similar to the reasons that the rejection of independent claims 1 and 12 are in clear error.

CONCLUSION

It is respectfully submitted that Examiner's rejections are in clear error and that this application is in condition for allowance. Notice to that effect is earnestly solicited.

Respectfully submitted,
BEYER WEAVER & THOMAS, LLP


Michael J. Ferrazano
Reg. No. 44,105

P.O. Box 70250
Oakland, CA 94612-0250
(650) 961-8300